IN THE CLAIMS

Claim 1 (Previously Presented): An information-processing apparatus for decrypting encrypted data stored on an information-recording medium, said information-processing apparatus comprising a plurality of encryption-processing units, comprising:

first generating means for generating a first block key Kb1 on the basis of a first seed serving as key generation information set for the encryption-processing unit;

acquiring means for acquiring a second seed by decrypting an encrypted second seed read out from said information-recording medium on the basis of said generated first block key Kb1;

second generating means for generating a second block key Kb2 by encrypting based on said acquired second seed; and

decrypting means for decrypting said encrypted data read out from said information-recording medium based on said generated second block key Kb2.

Claim 2 (Previously Presented): The information-processing apparatus according to claim 1, said information-processing apparatus including storage means for storing master-key generation information, wherein

master key generating means generates a master key on the basis of said master-key generation information,

recording key generating means generates first recording key K1 and second recording key K2 on the basis of said generated master key and information read out from said information-recording medium,

said first generating means generates said first block key Kb1 by encrypting based on said generated first recording key K1 and said first seed,

said acquiring means acquires said second seed by decrypting said encrypted second seed read out from said information-recording medium on the basis of said generated first block key Kb1,

said second generating means generates said second block key Kb2 by encrypting based on said acquired second seed and said generated second recording key K2, and

decoding means decodes said encrypted data read out from said information-recording medium by decrypting based on said generated second block key Kb2.

Claim 3 (Previously Presented): The information-processing apparatus according to claim 2 wherein

unique key generating means generates a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and two title keys recorded on said information-recording medium, and

said recording key generating means generates said first recording key K1 by encrypting based on said first title unique key and first information read out from said information-recording medium, and generates said second recording key K2 by encrypting based on said second title unique key and second information read out from said information-recording medium.

Claim 4 (Previously Presented): The information-processing apparatus according to claim 2 wherein said encryption-processing means further comprises:

unique key generating means generates a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said

information-recording medium, and one key seed recorded on said information-recording medium, and

said recording key generating means generates said first recording key K1 by encrypting based on said first title unique key and first information read out from said information-recording medium, and generates said second recording key K2 by encrypting based on said second title unique key and second information read out from said information-recording medium.

Claim 5 (Previously Presented): An information-recording medium drive configured to read out encrypted data from an information-recording medium and output said encrypted data to an external apparatus, said information-recording medium drive comprising:

an authentication-processing unit configured to carry out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

a plurality of encryption-processing units, at least one encryption-processing unit configured to:

generate a first block key Kb1 on the basis of a first seed serving as key generation information set for the encryption-processing unit,

acquire a second seed by reading out and decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1, and

generate output-use encrypted information by encrypting data including said second seed on the basis of said session key Ks, wherein said output-use encrypted information obtained as a result of said process to encrypt data including said second seed on the basis of said session key Ks is output through an interface.

Claim 6 (Previously Presented): The information-recording medium drive according to claim 5 wherein each encryption-processing unit is further configured to:

generate a master key on the basis of master-key generation information held by said information-recording medium drive;

generate two recording keys K1 and K2 on the basis of said master key and information read out from said information-recording medium;

generate the first block key Kb1 by carrying out an encryption process based on said generated first recording key K1 and said first seed;

acquire the second seed by decrypting the encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generate the output-use encrypted information by encrypting data including said second seed and said second recording key K2 on the basis of said session key Ks; and

output said output-use encrypted information including said second seed and said second recording key K2 through an interface.

Claim 7 (Previously Presented): An information-processing apparatus for decrypting encrypted data received from an external apparatus through a data input interface using encrypted information received through said data input interface, said information-processing apparatus comprising:

an authentication-processing unit for carrying out an authentication process with said external apparatus outputting said encrypted data in order to generate a session key Ks; and

an encryption-processing unit for:

acquiring a seed used as key generation information and a recording key by decrypting, based on said session key, said encrypted information received through said data input interface,

generating a block key to be used as a decryption key for decryption of said encrypted data by encrypting, based on said seed and said recording key, and

decrypting, based on said block key, said encrypted data.

Claim 8 (Previously Presented): An information-recording medium drive for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-recording medium drive comprising:

an authentication-processing unit for carrying out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

a plurality of encryption-processing units, at least one encryption-processing unit comprising:

means for generating a block key on the basis of a seed serving as key generation information set for the encryption-processing unit;

means for acquiring decrypted data by decrypting said encrypted data read out from said information-recording medium on the basis of said generated block key; and

means for generating output-use encrypted information by encrypting said decrypted data on the basis of said generated session key Ks,

wherein said output-use encrypted information obtained as a result of said encrypting of said decrypted data on the basis of said session key Ks is output through an interface.

Claim 9 (Previously Presented): A method of manufacturing an information-recording medium used for storing encrypted data, said method comprising:

generating, outside the information-recording medium, a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data;

storing said first seed in the information-recording medium;

generating, outside the information-recording medium, a second seed serving as key generation information encrypted on the basis of a first block key Kb1 generated on the basis of said first seed;

storing said second seed in the information-recording medium;

generating, outside the information-recording medium, an encrypted content encrypted on the basis of a second block key Kb2 generated on the basis of said second seed; and

storing said encrypted content in the information-recording medium.

Claim 10 (Previously Presented): The method according to claim 9 wherein said first seed is stored inside control information set for each of encryption-processing units whereas said second seed is stored as encrypted information in a user-data area outside said control information.

Claim 11 (Previously Presented): The method according to claim 9 wherein said first seed is stored in a user-data area as unencrypted data whereas said second seed is stored in said user-data area as part of said encrypted data.

Claim 12 (Previously Presented): The method according to claim 9 wherein said encrypted data is a transport stream packet, said first seed is stored inside control information for a plurality of transport stream packets, and said second seed is stored as encrypted

information inside one of said transport stream packets in a user-data area outside said control information.

Claim 13 (Previously Presented): The method according to claim 9 wherein said first seed is stored inside a transport stream packet in a user-data area as unencrypted data whereas said second seed is stored as encrypted information inside said transport stream packet in said user-data area.

Claim 14 (Previously Presented): An information-processing method for decrypting encrypted data stored on an information-recording medium, said information-processing method comprising:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of a plurality of encryption-processing units including said encrypted data stored on said information-recording medium;

acquiring a second seed by decrypting an encrypted second seed read out from said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 based on said acquired second seed; and

decrypting said encrypted data read out from said information-recording medium by decrypting, based on said generated second block key Kb2.

Claim 15 (Previously Presented): The information-processing method according to claim 14, said information-processing method further comprising:

generating a master key on the basis of master-key generation information read out from storage means;

generating two recording keys K1 and K2 on the basis of said generated master key and information read out from said information-recording medium;

generating said first block key Kb1 by encrypting, based on said generated first recording key K1 and said first seed;

acquiring said second seed by carrying out a process to decrypt an encrypted second seed read out from said information-recording medium on the basis of said generated first block key Kb1;

generating said second block key Kb2 by encrypting, based on said acquired second seed and said generated second recording key K2; and

decrypting said encrypted data stored on said information-recording medium by decrypting, based on said generated second block key Kb2.

Claim 16 (Previously Presented): The information-processing method according to claim 15, said information-processing method further comprising:

generating a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and two title keys recorded on said information-recording medium;

generating said first recording key K1 by encrypting, based on said first title unique key and first information read out from said information-recording medium; and

generating said second recording key K2 by encrypting, based on said second title unique key and second information read out from said information-recording medium.

Claim 17 (Previously Presented): The information-processing method according to claim 15, said information-processing method further comprising:

generating a first title unique key and a second title unique key on the basis of said master key, a disc ID, which is information read out from said information-recording medium, and one key seed recorded on said information-recording medium;

generating said first recording key K1 by encrypting, based on said first title unique key and first information read out from said information-recording medium; and

generating said second recording key K2 by encrypting, based on said second title unique key and second information read out from said information-recording medium.

Claim 18 (Previously Presented): An information-processing method used for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-processing method comprising:

carrying out an authentication process with said external apparatus to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks; and

generating, outside said information-recording medium, a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units composing said encrypted data stored on said information-recording medium;

acquiring a second seed, outside said information-recording medium, by decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating output-use encrypted information by encrypting data including said second seed on the basis of said session key Ks; and

outputting said output-use encrypted information obtained as a result of encrypting data including said second seed on the basis of said session key Ks through an interface.

Claim 19 (Previously Presented): The information-processing method according to claim 18, said information-processing method further comprising:

generating a master key on the basis of master-key generation information held by an information-recording medium drive;

generating two recording keys K1 and K2 on the basis of said master key and information read out from said information-recording medium;

generating said first block key Kb1 by encrypting, based on said generated first recording key K1 and said first seed;

acquiring said second seed by decrypting an encrypted second seed stored on said information-recording medium on the basis of said generated first block key Kb1;

generating said output-use encrypted information by encrypting data including said second seed and said second recording key K2 on the basis of said session key Ks; and

outputting said output-use encrypted information including said second seed and said second recording key K2 through an interface.

Claim 20 (Previously Presented): An information-processing method used for carrying out a process to decrypt encrypted data received from an external apparatus through a data input interface using encrypted information received from said data input interface, said information-processing method comprising:

carrying out an authentication process with said external method outputting said encrypted data in order to generate a session key Ks;

acquiring a seed used as key generation information and a recording key by decrypting, based on said session key, said encrypted information received through said data input interface;

generating a block key to be used as a decryption key for decryption of said encrypted data by encrypting, based on said seed and said recording key; and

decrypting said encrypted data.

Claim 21 (Previously Presented): An information-processing method used for reading out encrypted data from an information-recording medium and outputting said encrypted data to an external apparatus, said information-processing method comprising:

carrying out an authentication process with said external method to receive said encrypted data read out from said information-recording medium in order to generate a session key Ks;

generating a block key on the basis of a seed serving as key generation information set for each of a plurality of encryption-processing units;

acquiring decrypted data by reading out and decrypting encrypted data stored on said information-recording medium on the basis of said generated block key;

generating output-use encrypted information by encrypting said decrypted data on the basis of said generated session key Ks; and

outputting said output-use encrypted information obtained as a result of said process to encrypt said decrypted data on the basis of said session key Ks through an interface.

Claim 22 (Previously Presented): A computer-readable storage medium configured to store a program, which, when executed, performs a method of decrypting encrypted data stored on an information-recording medium, said method comprising:

generating a first block key Kb1 on the basis of a first seed serving as key generation information set for each of encryption-processing units;

acquiring a second seed by decrypting an encrypted second seed read out from said information-recording medium on the basis of said generated first block key Kb1;

generating a second block key Kb2 based on said acquired second seed; and

decrypting said encrypted data stored on said information-recording medium by decrypting, based on said generated second block key Kb2.